INTRODUCTION TO SECURITY/OPERATION SECURITY

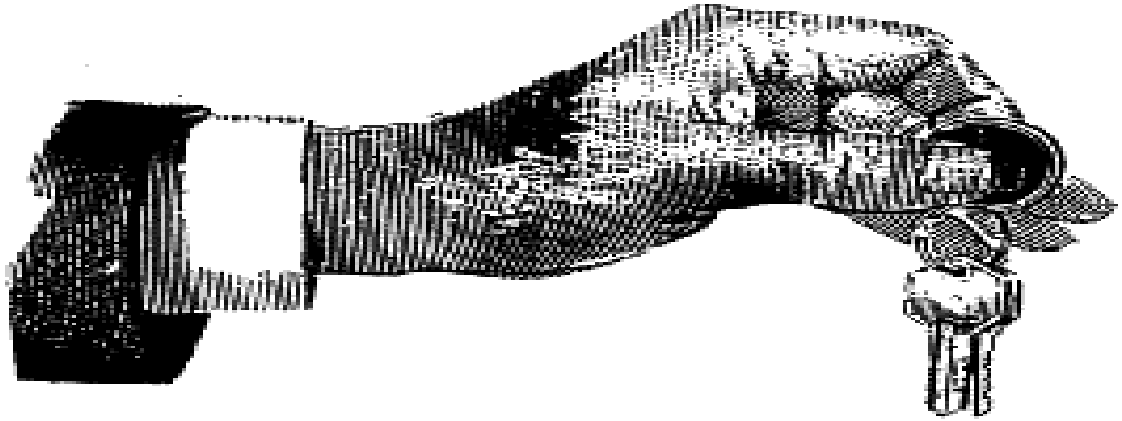
Navy Personnel Command

SECURITY BRANCH

SECURITY BRANCH

SECURITY Branch (PERS-334) is located in Wood Hall, Building 769, Room 184

KEY ELEMENTS OF SECURITY



The *"KEY"* elements of a *GOOD* security program include:

Information Security

Personnel Security

Physical Security

Industrial Security

SECURITY MANUALS

- SECNAVINST 5510.30A
- SECNAVINST 5510.36
- SECNAVINST 5239.3
- OPNAVINST 5239.1B
- OPNAVINST 5530.15A
- BUPERSINST 5239.1B
- NAVPERSCOMINST 5530.1A
- NAVPERSCOMINST 5510.1
- DODD 5205.2
- OPNAVINST 3432.1

PERSONNEL SECURITY

- **All personnel (civilians, military and contractors) at NPC must possess a valid security investigation consistent with the interests of National Security per SECNAVINST 5510.30A**

ACCESS TO CLASSIFIED INFORMATION

- **Appropriate Clearance**
  - **Adjudicated for specific level of Classified information (Top Secret, Secret, Confidential)**
- **Approved Access**
  - **Authorized by PERS-334**
- **Need to Know**
  - **Job Requirement**

CLASSIFIED INFORMATION

- **Handling Procedures**
  - **Store classified diskettes and removable media in appropriate approved security safes when not in use**
  - **Dispose/destroy printed materials and data as prescribed in SECNAVINST 5510.36**
  - **Do not discuss classified information in an Unclassified/unsecured environment (Telephone)**
  - **Never remove classified information from command without authorization from Command Security Manager**

CLASSIFIED INFORMATION (CON'T)

- **Never reveal classified information to anyone without ensuring they are properly cleared, have access, and have a need-to-know**
- **Never reproduce classified information without proper authorization**
- **Make sure reproduction is done on authorized copier machine for level of classification**
- **Do not put classified information on command LAN (PERSNET) or Navy Marine Corps Internet (NMCI)**
- **Only use SIPRNET or Secure Fax to transmit classified information**

COMPROMISE

- **Loss of classified information that cannot be physically located or accounted for**
- **Classified information placed and routed in guard mail envelopes or on unclassified LAN**
- **Unauthorized disclosure**
- **Classified information not properly controlled and stored**
- **Report any loss or compromise of classified information to Command Security Manager at 4-3091 immediately**

MAILING CLASSIFIED INFORMATION

- **SECNAVINST 5510.36 provides the procedures for mailing classified information**
- **Any questions call PERS-334**

PICKUP AND RELEASE MESSAGE TRAFFIC

- **Authorized by PERS-334**
- **Classified messages are picked up in person at the message center**
- **All classified messages must have a cover sheet to identify classification and be carried in a briefcase, envelope or folder to prevent viewing**
- **Department Security Assistant's are responsible for maintaining accountability on distribution and destruction of classified messages for their department**

INFORMATION SECURITY

- BUPERSINST 5239.1B
- Use of personal computer software or hardware is not authorized on any BUPERS system
- NO desk top modems authorized
- Use of computer games is prohibited
- Incident reporting - particularly virus

INFORMATION SECURITY (CON'T)

- **Only Navy Marine Corp Internet (NMCI) personnel can move your government computer. You must put in a Move, Add and Change (MAC) request through your ISSO**
- **If you use a classified computer, make sure all your diskettes are marked and labeled properly**
- **Use your government computer for Official Business Only**
- **Make back-ups if required**
-

USER RESPONSIBILITY AGREEMENT

- **Use desktop screen saver passwords**
- **Do not give your computer password to anyone under any circumstances**
- **If you forget your password, locked out of the system or have any problems with your computer system, you must contact NMCI at 1-866-843-6624**
- **If you are on a Legacy (PERSNET) system contact your ISSO or the Information Systems Security Manager, Ms. Regina Miller, 4-4942**
- **Do not write your password down, stick it in your wallet, rolodex or tape it under your keyboard**

USER RESPONSIBILITY AGREEMENT (CON'T)

- **Obey all command Intranet/Internet policies**
- **Do not try to circumvent security requirements to obtain unauthorized access**
- **If issued a laptop, safeguard it. Do not leave unsecured**
- **Do not change configuration of any command network component, including laptops**

DOD WARNING BANNER

UNITED STATES DEPARTMENT OF DEFENSE WARNING STATEMENT

This is a Department of Defense Computer system. This computer system including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

PHYSICAL SECURITY

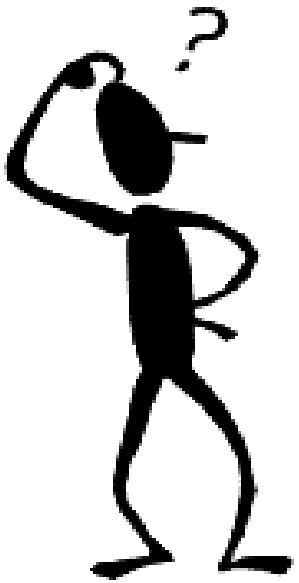
- **Ensure only authorized individuals have access to safes containing classified information**
- **Use SF-701, Activity Security Checklist, for spaces storing classified information**
- **Use SF-702, Security Container Check Sheet, when opening and closing safe**
- **Ensure SF-700, Security Container Information form, is completed and taped inside safe to display authorized personnel with access to safe**
- **Ensure OF-89, Maintenance Record, is taped on the inside of safe**

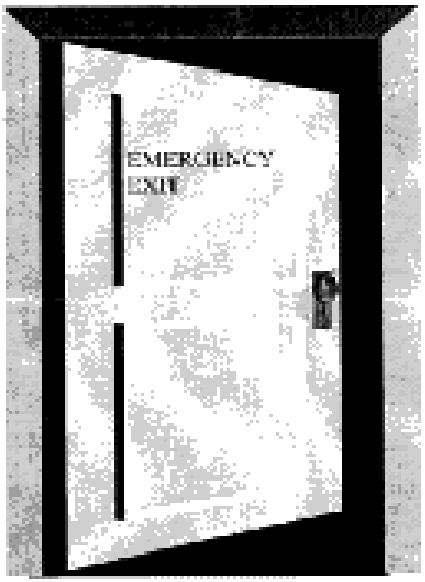
PHYSICAL SECURITY (CON'T)

- **Video Badging System - creates and encodes ID badges for personnel access to command buildings and spaces**
- **Access Control System - reads the badge and controls entry points**
- **Intrusion Detection System - monitors numerous sensors and notifies security when alarm is activated**

PHYSICAL SECURITY (CON'T)

DO NOT GO OUT EMERGENCY EXIT DOORS UNLESS IT IS AN EMERGENCY..





INDUSTRIAL SECURITY

- DOD 5220.22-M
- Contractor Personnel

OPERATION SECURITY (OPSEC)

- OPSEC is a risk management tool used to deny an adversary information generally unclassified but critical/sensitive concerning our intentions and capabilities

OPSEC (CON'T)

- WHAT IS CRITICAL/SENSITIVE INFORMATION?
  - Information about our activities, intentions and capabilities, that an adversary needs to gain an advantage

OPSEC (CON'T)

- EXAMPLES OF CRTICAL/SENSITIVE INFORMATION
  - Troop Deployment
  - Weapon Systems Technology
  - Local Exercises
  - Test Schedules

OPSEC (CON'T)

- WHO IS AN ADVERSARY?
  - **International Terrorists Groups**
  - **Foreign Intelligence Agencies**
  - **Hackers and Crackers**
  - **Other Types of Adversaries**
    - **Disgruntled Employees**
    - **Dishonest Employees**

OPSEC (CON'T)

- **HOW IS THIS INFORMATION COMMUNICATED?**
  - Internet
  - Cellular Phones
  - Fax Machines
  - Unsecured Communication Lines

OPSEC (CON'T)

- **RULES FOR EFFECITVE OPSEC**
  - **Don't discuss readiness Issues**
  - **Don't discuss specific training exercises**
  - **Don't assume the enemy is not trying to collect information**

OPSEC (CON'T)

- **KEY POINTS**
  - **GOOD OPSEC SAVE LIVES AND RESOURCES**
  - **ALWAYS USE COMMON SENSE AND BE AWARE**
  - **LOOK AT PROCEDURES FOR DESTRUCTION OF SENSITIVE INFORMATION**

SECURITY/MAIL DIVISION WEBSITE

- Visit the Security Web site on the NPC Intranet under ADMINISTRATION for additional security and mail information

BOTTOM LINE

- SECURITY IS AN ALL HANDS ISSUE

THINK SECURITY!!!

QUESTIONS?

- **My time is up, Thank You.**
- **SHOW VIDEO**